Data Acquisition: No Limits

How digital wireless technology using the IEEE802.15.4 ZigBee standard is helping datalogging applications break free

Mark Lee

The consumer electronics market has seen an explosion of gadgets enabled by wireless technology over the past 5 years, with the wide uptake of devices such as wireless broadband routers, Bluetooth headsets, DECT phones and audio-visual senders. The commercial market has been far more cautious in embracing these technologies when designing environmental monitoring and process control systems, with concerns over reliability, data security and potential cost outweighing the obvious convenience benefits.

With an increasing demand for easy, flexible environmental monitoring systems in sensitive sites such as museums, healthcare manufacturers and heritage listed buildings, the massive advantages offered by new wireless technology are becoming impossible to ignore when specifying data acquisiton systems.

Cables?

Local and high speed data acquisition has historically been a case of connecting sensors to a data logging device to a PC or PLC, via cable. Cables typically offer a guaranteed, reliable point-to-point connection, several decades of reliable service, and high bandwidth capacity resulting in large amounts of dataflow at high speed.

Long cable runs to remote sensors around a site however, suffer from two main problems. The first is disruption to the building fabric and operation if new cable routes have to be laid to install the system, and subsequent further disruptive work if the system needs to be modified, or sensors added or moved.

The second major problem is one of maintaining signal integrity over long cable runs. All cables are subject to interference from nearby strong magnetic fields and signal decay (where the measured signal at the sensor end fades along the length of the cable, changing the measurement). Active repeaters, amplifiers and filters are common processes used to try to boost signal-to-noise ratio (SNR), often with mixed success.

Wireless!

Wireless data acquisition makes installation as easy as placing sensors in the correct locations, then adding or moving them if the system needs to be modified. It also overcomes the problem of maintaining signal integrity by sampling and converting the analog measurement signals into digital data at the monitoring point ready for radio transmission. Wireless signals are of course just as prone to interference and

decay as wired signals, but with digital transmission, the carried data includes its own error checking and correction, and higher level protocols will manage the checking and re-sending of data should an interference to transmission occur. In addition, modern digital coding techniques allow much more information to be carried in the same bandwidth than would be the case with an analog signal.

Technology

The latest wireless environmental monitoring systems in Australia use the 2.4GHz radio band, available for home use and typically used by wireless routers, Bluetooth devices, AV senders and DECT phones. Rather than consumer protocols, commercial wireless monitoring systems use a high level protocol known as ZigBee, based on the IEEE 802.15.4 standard for wireless personal area networks (WPANS), which was ratified in 2004.

The ZigBee protocol was designed to be simpler, cheaper and more power efficient than other 2.4GHz technologies, with devices requiring significantly less programming code than Bluetooth and wireless LAN devices. This makes ZigBee radio nodes up to five times cheaper than similar Bluetooth devices – enabling great value for data acquisition systems requiring many wireless nodes.

Security

The ZigBee protocol was designed with built-in security as a top priority, unlike 802.11 wireless LANs or Bluetooth which suffer from several security weaknesses. While the 802.15.4 standard specifies the use of AES (Advanced Encryption Standard) encryption using up to 128-bit shared keys for secure transport, the ZigBee protocol defines the way the keys are established, and how nodes recognise and react to each other throughout the mesh network (authentication). The master network controller keeps a list of authenticated devices (those that have specifically joined the network in a process known as association), and only responds to these devices, blocking messages from foreign nodes.

The master also supervises the distribution of encryption keys to new nodes across already secure parts of the network. ZigBee network nodes can choose from three different types of key: master, network and link. The network key protects the entire network from outside intrusions, and the link key forms the basis of security between two devices. If the link key is available, it is always used. Nodes can use the less secure network key if required to conserve memory, but as this key is used across several devices it can be susceptible to insider attacks. End-to-end security is maintained from sender to receiver by encrypting the data once. Intermediate nodes do not decrypt and re-encrypt the packets, but only relay them on to their destination. Finally the network master also maintains a ‘freshness’ list, which assigns a unique counter id when each key is established. If the master detects messages it has already received (with ‘stale’ or out-of-synch freshness counters) it suspects a hacker is replaying or falsifying messages and chooses to ignore the intrusion.

Interference Robustness

The ZigBee network copes with potential interference from other 2.4GHz devices by scanning the radio environment for traffic, and selecting appropriate channels away from (or slotted between) competing signals. 802.11 devices have eleven 22MHz spread spectrum channels defined at a 25MHz spacing between 2.401GHz and 2.473GHz. ZigBee devices however have 26 narrower (3MHz) channels at 5MHz spacing defined in the same frequency range, meaning lower bandwidth channels, but far greater scope to find an unused portion of the spectrum to communicate in.

Networking

ZigBee devices form a mesh network, allowing devices to relay messages from a more distant node to the network's central base station. This significantly extends the range of the system from a basic point-to-point range of 80m, to a maximum network range of 1.2km, and allows messages to find different routes through the system when certain nodes become unavailable for any reason. This mesh packet network concept is so powerful and robust it forms the basis of the entire internet, a firm foundation for a reliable wireless data acquisition system.

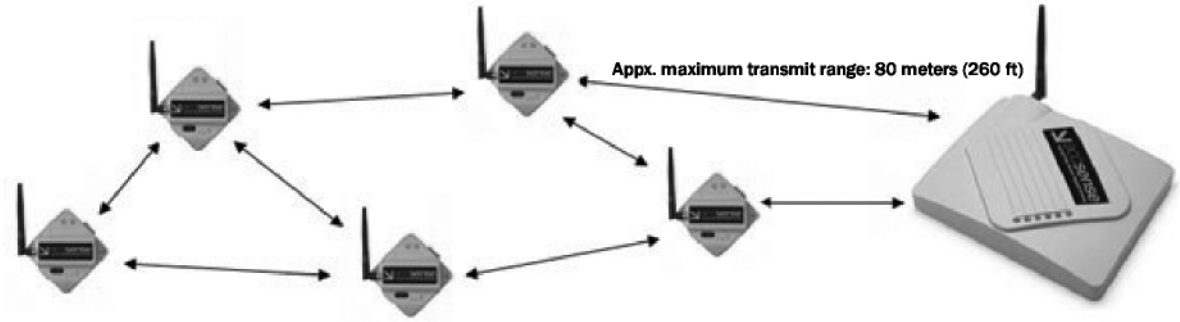

Figure x – The wireless 'mesh' network allows the system's range to be extended by repeating signals

Considering the Operating Environment

When new wireless data acquisition systems are planned, an initial site survey should be carried out, which takes into account how the wireless signal will propagate from the wireless nodes to the base station. Factors such as whether the wireless signal has to travel through walls, glass, doors, or openings must be taken into account, all of which effectively attenuate the wireless signal and reduce the range. Attenuations encountered can be added to produce a power budget and determine whether the site for a particular node is viable, or whether the site requires enhanced antennas or cabling.

Items to losses to be added	dB
Human body	3
Cubicles	3 to 5
Marble	5
Window, Brick Wall	2

Clear Glass Window	2
Office window	3
Glass wall with metal frame	6
Metal Screened Clear Glass Window	6
Wired-Glass Window	8
Brick Wall next to a Metal Door	3
Plasterboard wall	3
Cinder block wall	4
Dry Wall	4
Sheetrock/Wood Frame Wall	5
Sheetrock/Metal Framed Wall	6
Office Wall	6
Brick Wall	2 to 8
Concrete Wall	10 to 15
Wooden Door	3
Metal door	6
Metal Door in Office Wall	6
Metal door in brick wall	12 to 13

Table 1 – Attenuation losses for common indoor obstacles

Data acquisition nodes based on ZigBee have a standard range of 80m in free air with -1dBm at the transmitter, -94dBm receiver sensitivity, and a standard 2.2dBi antenna (as found on wireless routers). The range can be extended with a higher gain antenna, every 6dB of gain introduced into the system giving an effective doubling of the range in free air. The wireless mesh can be extended into potentially radio 'dead' locations, such as underground tunnels and store rooms using custom designed combinations of antennae and cabling.

Information Flow

In the latest wireless data acquisition products, nodes with internal sensors capable of measuring temperature, humidity, light level, sound and vibration and dew point are available. Nodes also have additional analogue inputs which accept industry-standard 0-5V and 4-20mA signals suitable for connecting external sensors, and digital inputs suitable for measuring contact closure, counting and totalising events.

The sampled data is fed from the nodes back to a base station, which coordinates the acquisition from all nodes at set time intervals, gathers the measurements and feeds them back to a database or PC-based application via standard ethernet. If the base station is required at a location with no local network available, GPRS based wireless modems can be used and the signals transmitted across mobile phone networks, allowing for a truly remote monitoring system.

Network Robustness

If communication is lost from node to base station the node can buffer data until the line is restored, and similarly data buffering is available at the base station if the network is interrupted for any period of time. Once the data has been fed into a PC-based enterprise system backed up with a database, every measurement, system

configuration change, alarm activated and acknowledged is logged and traceable, providing a unique and compliant data acquisition system.

Hard To Ignore

With customers' demands for easy, unobtrusive, flexible data acquisition driving the development of high specification wireless data acquisition and monitoring systems, it seems that wireless devices are no longer just 'gadgets' for the consumer electronics market – they have a powerful role to play in demanding data acquisition applications.

Mark Lee is a Technical Specialist for Neo Vista Systems Integrators Pty Ltd.(NVSI) of Sydney, Australia and Auckland, New Zealand (www.nvsi.com.au).
Mark studied wireless digital communications systems at Bristol University in the UK, and has worked with National Instruments data acquisition products since 2004.

NVSI are the developers and distributors of the Enviropoint wireless monitoring system powered by Accsense.
For more information please call (02) 9809 7899 or e-mail info@nvsi.com.au